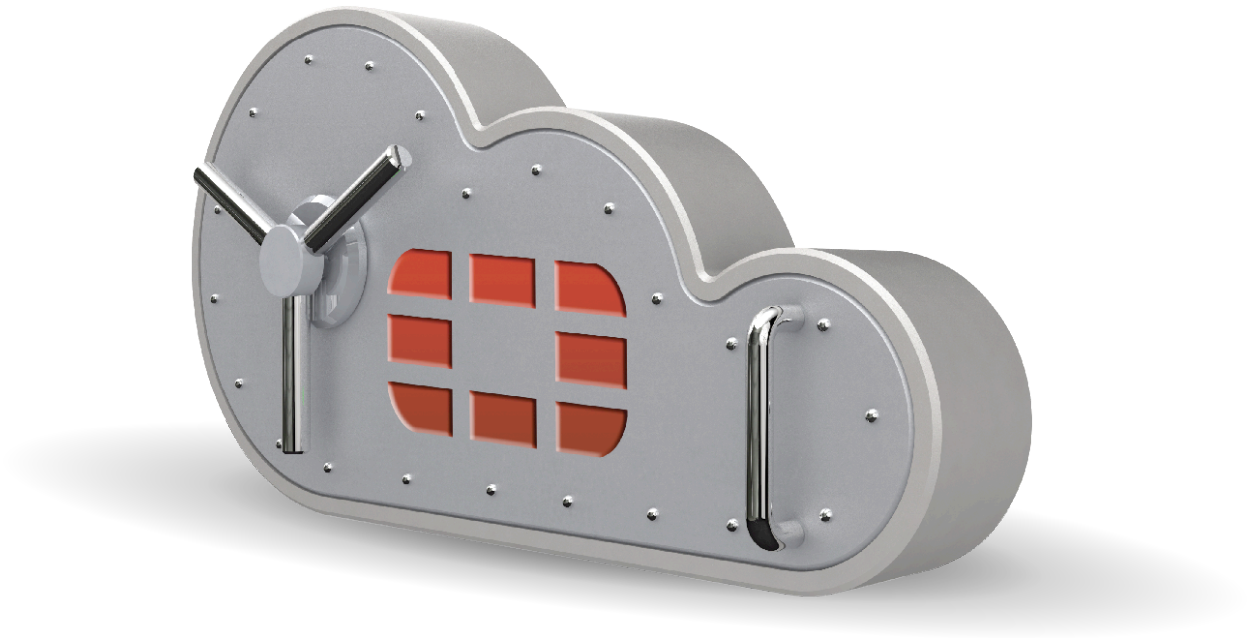
WHITE PAPER

FortiMail Identity Based Encryption

A Business and Compliance Enabler



Contents

Business Need Secure Mail Delivery

Email has evolved into one of the most important methods of communication for any organization. However, email was never created with security in mind which creates abundant opportunities for misuse and fraud -- every non-encrypted email sent over a network can be read, copied or altered during transmission.

There is a strong business need for secure mail delivery:

- Industries such as healthcare, finance and government must comply with regulations to protect sensitive data in electronic communication
- Secure mail delivery significantly reduces the costs associated with printing, faxing and overnight delivery of paper-based communication
- Secure mail delivery enables online business channels as it facilitates sharing confidential, regulated, or proprietary information with customers, employees, clients and partners in safe, secure manner

Challenges with Available Technologies

The most popular tools available today for secure messaging are Secure/Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP) encrypted communication, and Transport Layer Security (TLS) secure connections. In spite of their popularity, these technologies each present significant operational challenges to organizations wishing to deploy encrypted messaging.

Transport Layer Security (TLS/SSL)

SMTP communication between mail servers can be secured using transport layer security methods e.g. TLS/SSL. This is a relatively simple method to set up however, it has some limitations:

- Communication channel is encrypted between the sender and recipient mail servers but the mail itself is not encrypted between the server and the end user
- TLS encryption is dependent on the remote server also supporting TLS and having it correctly configured
- If TLS/SSL is not available, communication will commonly default to unencrypted

S/MIME

S/MIME is a standard for public key encryption and signing of MIME data. It was originally developed by RSA Data Security, Inc. to provide cryptographic security services for electronic messaging applications including authentication, message integrity and non-repudiation of origin (using digital signatures), and privacy and data security (using encryption). Before S/MIME can be used in any of the above applications, one must obtain and install an individual key/certificate either from one's in-house certificate authority (CA) or from a public CA.

However, there are many obstacles to deploying S/MIME in practice. First, not all e-mail software supports S/MIME signatures, resulting in an attachment called smime.p7s that may confuse recipients. Second, S/MIME is not supported for most web-based email clients, such as Gmail, Hotmail. Third, S/MIME is tailored for end-to-end security which introduces the drawback of encrypting not only the message, but also any malware, defeating the purpose of Firewall which normally sits at the company gateway and won't be able to identify the encrypted malware. Last but not least, some users don't take advantages of S/MIME because of the administrative overhead of issuing, maintaining, and revoking certificates.

PGP

Pretty Good Privacy (PGP) is a data encryption and decryption computer program and is often used for signing, encrypting, and decrypting emails to increase the security of email communications. PGP is a hybrid solution; it ties together the advantages of public key and symmetric cryptography by combining the convenience of public-key encryption with the fast speed of symmetric encryption.

While PGP is considered a better practice than S/MIME among security professionals, it does have its disadvantages:

- Complexity – using PGP can be a complex process and its implementation is often difficult.
- Compatibility – it is impossible to use PGP unless people at both ends of the connection are using the same version of PGP
- Key management – managing keys can be challenging for users who are new to PGP. Keys that are lost or corrupted can be a security risk to users in a highly secure environment

In summary, overall usability is as important a consideration as security. The certificate and key management challenges described above prevent organizations from deploying PGP and S/MIME to all users. Any encryption solution that is difficult to deploy and use will result in limited deployments and end-users avoiding the tools' usage, which results in poor practices and potential exposure for the organization. Organizations are looking for a secure mail encryption solution they can easily deploy and their users can readily adopt.

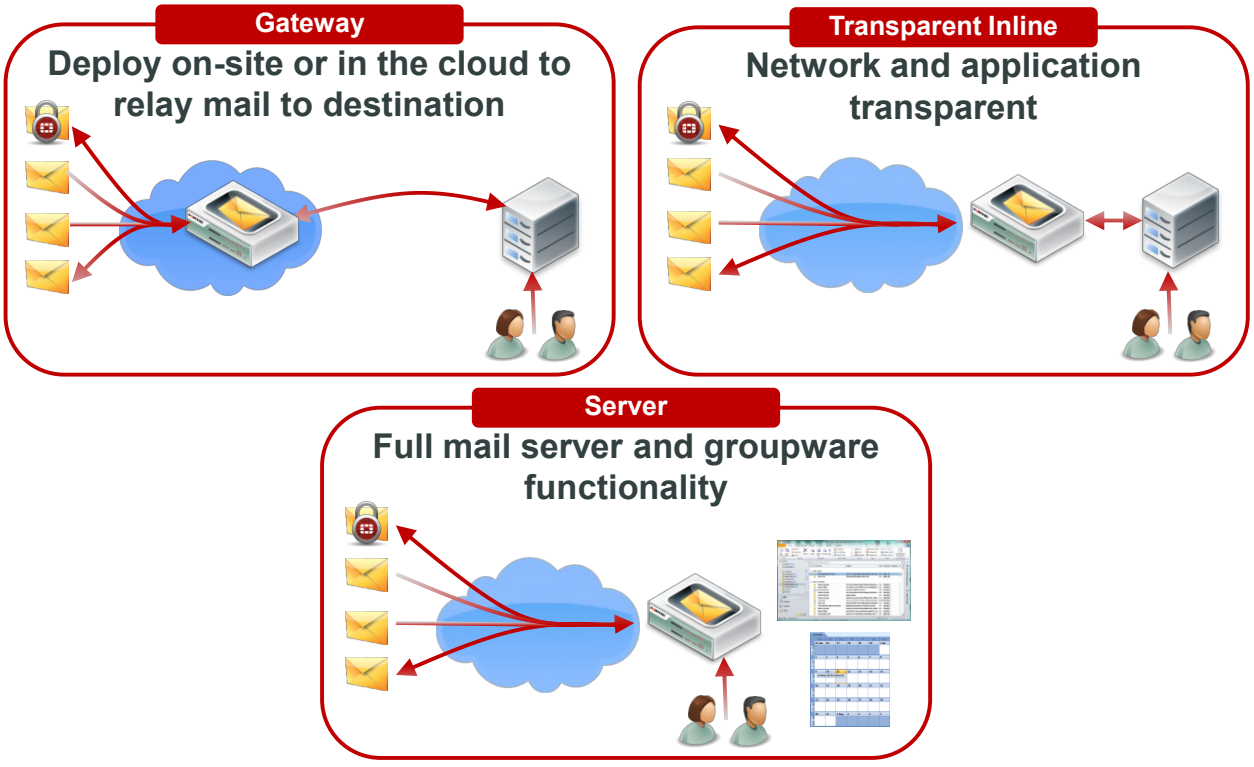
FortiMail Solutions

FortiMail Overview

Fortinet's FortiMail email security appliances are purpose-built antispam/antivirus systems that protect organizations of all sizes against message-borne threats. Its flexibility and versatility provide a turnkey approach to secure and clean corporate communication.

You can prevent your messaging systems from becoming threat delivery systems with FortiMail. Its inbound filtering engine blocks spam and malware before it can clog your network and affect users. Its outbound inspection technology prevents outbound spam or malware from causing other antispam gateways to blacklist your users (including mobile traffic). The FortiMail platform's dynamic and static user blocking gives you granular control over all of your policies and users.

Three deployment modes offer maximum versatility while minimizing infrastructure changes or service disruptions: transparent mode for seamless integration into existing networks with no changes to your existing mail server, gateway mode as a proxy MTA for existing messaging gateways, or full mail server functionality with POP3, IMAP and Webmail with groupware functionality.



FortiMail Identity-Based Encryption

FortiMail provides Identity-Based Encryption (IBE), in addition to S/MIME and TLS/SSL, as email encryption options to enforce policy-based encryption for secure content delivery. There are many benefits of using FortiMail IBE:

- **Security** – FortiMail IBE can be used in conjunction with any other services provided by FortiMail, such as antispam, antivirus and content filtering, to provide an extra layer of email protection.
- **Easy to use** – FortiMail IBE is as easy to use as a standard email. There is no need of certificate and key management for end-users and no need to install additional hardware or software. The recipient does not have to generate key pairs in order to read the encrypted document. No end-user provisioning and pre-enrollment requirements eliminate the need for end-user training and maintenance costs. FortiMail IBE enhances data security without impacting your productivity.
- **Flexibility** – FortiMail is one of the very few products on the market that offer IBE in both Push and Pull delivery options, delivering encrypted emails directly to your users, or storing them on the FortiMail platform for retrieval, or a combination of the two options.
- **Reduces Cost** – Eliminates the per-letter cost and environmental impact of paper-based communications. According to the Direct Marketing Association[1], the approximate cost for 100,000 pieces of direct mail is $1.00 per letter. Replacing 100,000 letters to its customers a year with FortiMail secure mail delivery will save approximately $100,000 yearly, and flow directly to the bottom line.
- **Lowers Total Cost of Ownership** – FortiMail IBE is available on all FortiMail appliances and in any mode of operation (Transparent, Gateway, and Server), without additional charges.

Identity-Based Encryption

How IBE Works

IBE is a type of public-key cryptography that uses unique information about the identity of the user to generate the public key. FortiMail uses a recipient's email address as well as other unique parameters (such as time stamp) to create the public key. You can enable automatic encryption of messages based on the attributes you choose, such as subject content, message body, or recipient domain. When an outbound email arrives at the FortiMail unit, it applies predefined policies to determine if the message requires encryption. Policies can be as simple as the user inserting a keyword into the subject e.g. [Encrypt] or an automatic detection of confidential content such as credit card or social security numbers or HIPAA, GLB or SOX content detected by lexical analysis. If there is a policy match, the FortiMail unit automatically triggers encryption of the message using the public key.

The recipient of the message can decrypt it regardless of his operating system, mail client or user privilege. A browser-based method allows the recipient to decrypt and read the secure message.

There is no need for additional software or the installation of any plug-in before FortiMail can send or receive an encrypted message. FortiMail secure mail delivery can interoperate with any email client, including Outlook, Lotus Notes, Thunderbird and Webmail such as Gmail, Yahoo, Hotmail etc.

Push and Pull for Secure Delivery

FortiMail offers two options to deliver encrypted messages – the Pull method and the Push method. The administrator has the flexibility to configure it to use either the push or the pull approach based on the message size. For instance, he can configure to use the Push approach for emails less than 1MB and use the Pull approach for emails greater than 1MB.

---

[1] www.the-dma-org.org

Pull Method (the encrypted email is stored on the FortiMail device)

1. The FortiMail device sends the recipient an email to notify that a new encrypted message is available.
2. Recipient clicks on the HTTPS link in the notification, which creates a web browser-based SSL connection with the originating FortiMail device.
3. The recipient authenticates with FortiMail (typically the recipient will authenticate via LDAP). The first-time user will have to register to create an account on the FortiMail local database.
4. The FortiMail issues the private key to decrypt the email and the user opens the encrypted email.

Please see Figure 1 for the detailed procedures of the Pull Method and Figure 3 for an example of the notification.

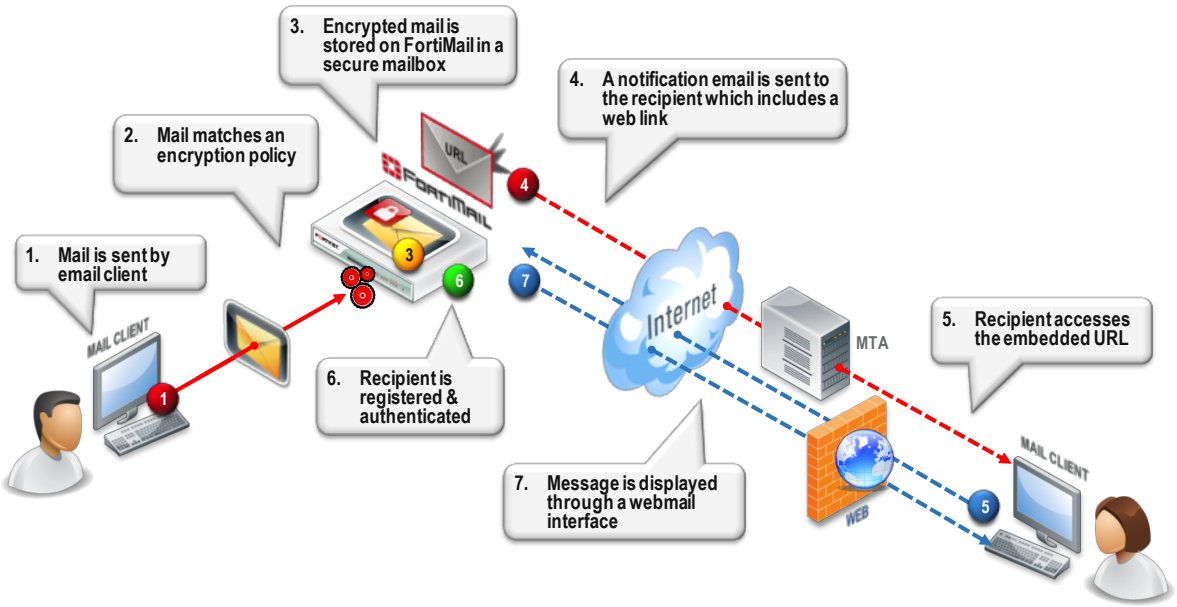


Figure 1: FortiMail IBE Pull Method

Push Method (the encrypted email is sent to the user)

1. The FortiMail sends the recipient a notification message with an encrypted HTML attachment.
2. The recipient clicks on the attachment (the encrypted message), which creates a web browser-based SSL connection with the originating FortiMail device.
3. The recipient's web browser "POSTs" the encrypted data in the attachment to the FortiMail for decryption.
4. The recipient authenticates with the FortiMail device (a first-time user will have to register to create an account).
5. The FortiMail decrypts the email, and the recipient reads and replies to the email.

Please see Figure 2 for the detailed procedures of the Push Method and Figure 3 for an example of the notification. The differences between the Push and Pull Methods are highlighted in yellow.

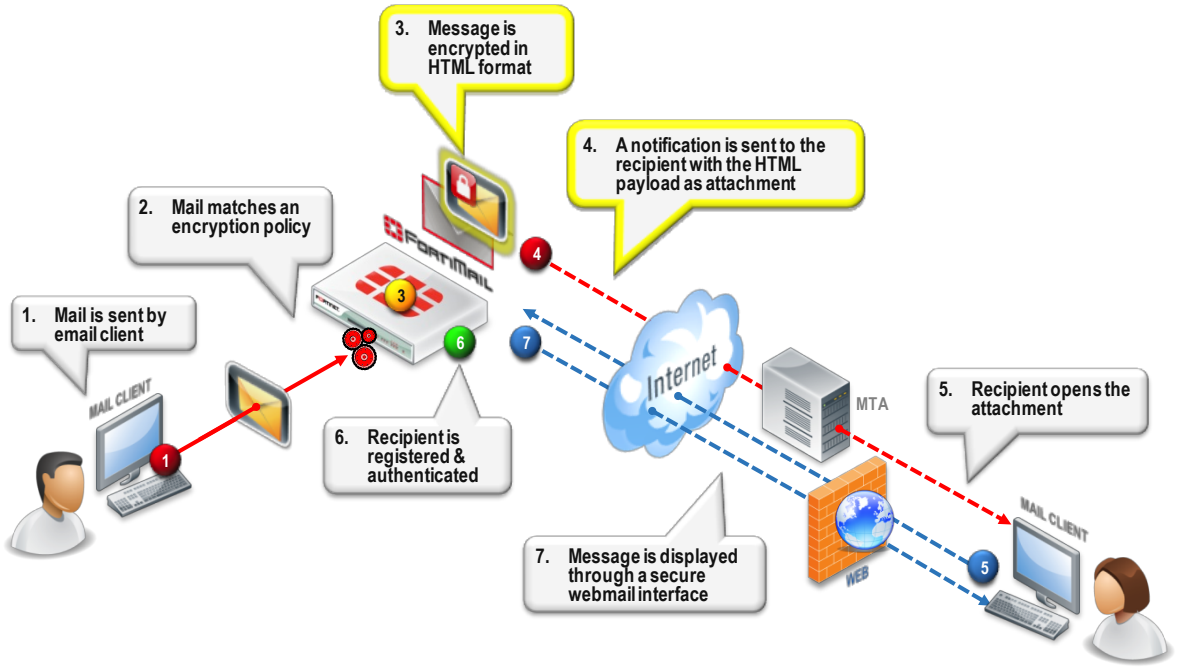


Figure 2: FortiMail IBE Push Method

Customized Notification

FortiMail IBE offers you the flexibility to customize the notification message in either HTML or plain text format. Please see Figure 3 for an example of the notification email for the Pull method, posting the encrypted payload as an HTTPS link to the FortiMail device, and an example for the Push method in HTML format, the encrypted payload is delivered as an attachment.

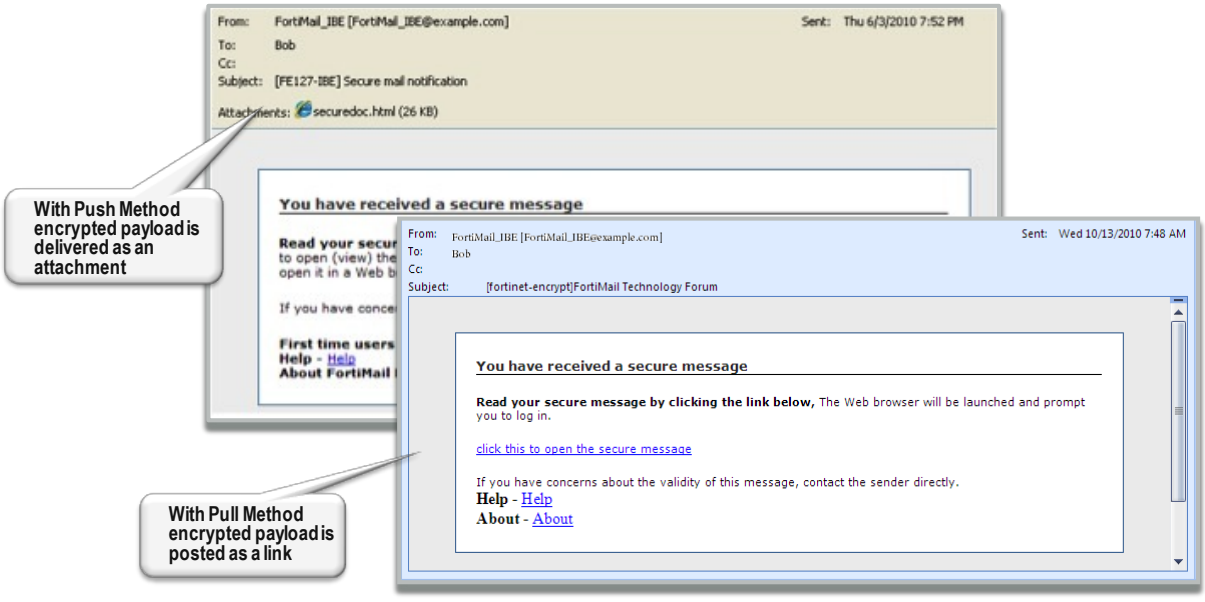


Figure 3: Notification Messages

IBE Encryption Options

FortiMail IBE supports encryption algorithms including 3DES, AES128, AES192, AES256 and CAST5 128. When the IBE server itself is unavailable, FortiMail provides alternative options to enforce TLS, drop and send DSN or send plain message. Please see Figure 4 for a screen shot on FortiMail management interface.

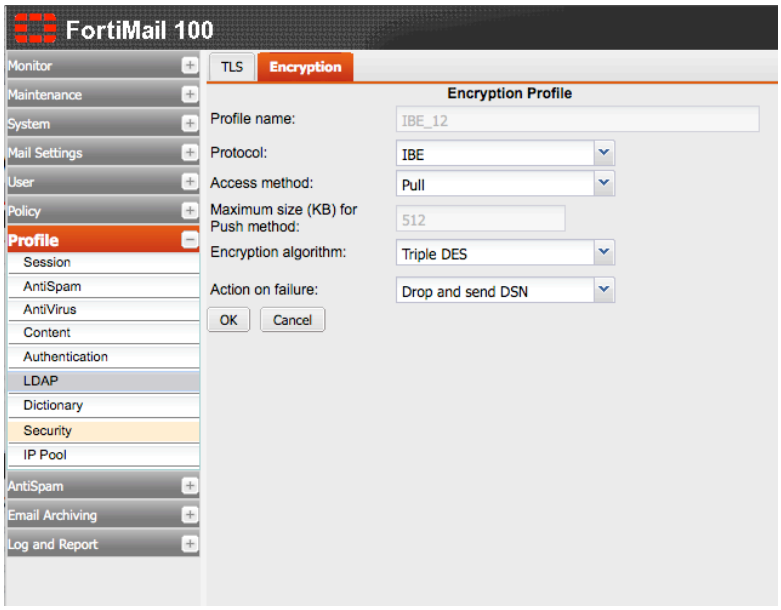


Figure 4: FortiMail Encryption Profile

User Enrollment and Secure Mail Access

IBE enrollment process doesn't require any administrative effort or maintenance. It uses the email address as the user's identity. User accounts can be stored on local FortiMail storage or an external NFS or iSCSI storage server. New users will have to complete a short online form for registration (Figure 5).

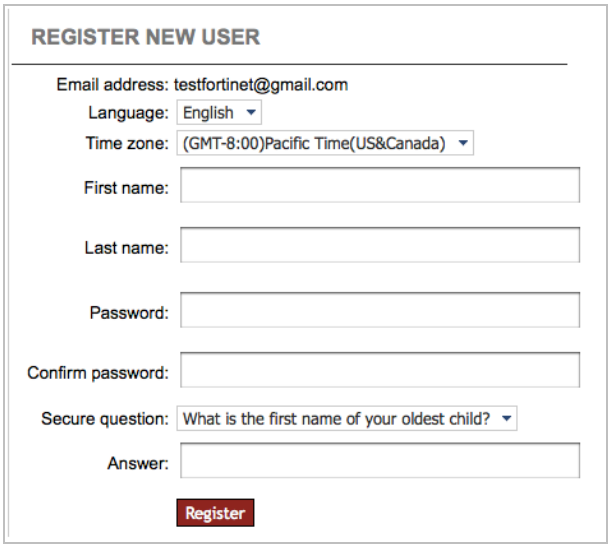


Figure 5: New User Registration Form

After successful enrollment, the recipient can manage secured emails on the FortiMail system. The administrator can customize the legal disclaimer and company logos. The interface is identical to the webmail interface in server mode. Please see Figure 6 for the screen shot.

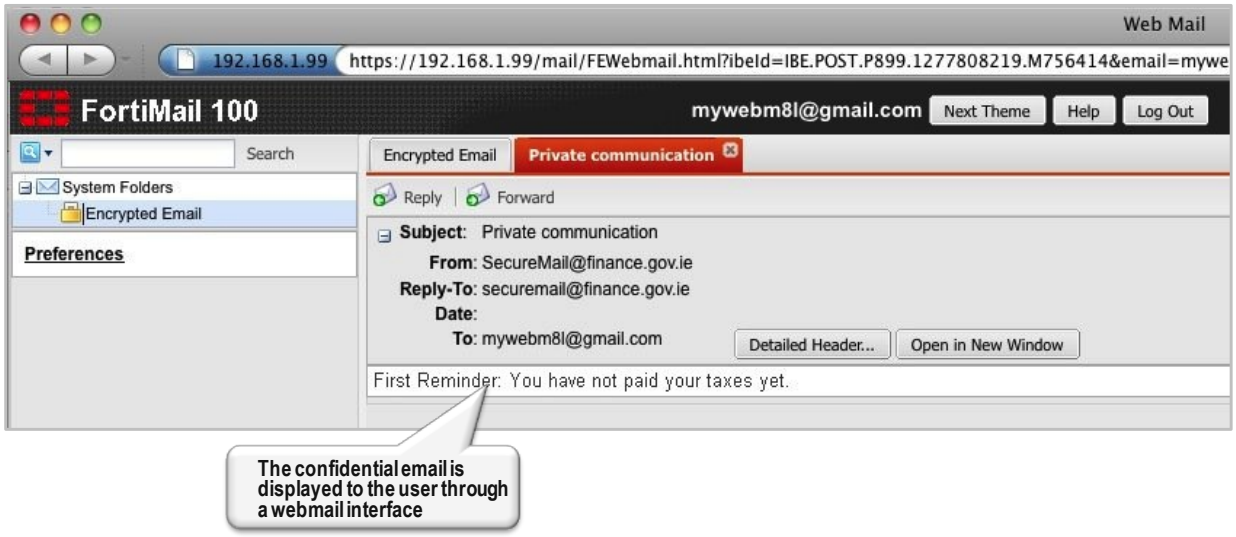


Figure 6 FortiMail Secure Mail Access

Deployment Options

You can assign mail storage, encryption, decryption and webmail access functions to a specific FortiMail unit. An optional deployment scenario is to configure a dedicated FortiMail unit as the centralized encryption and decryption unit. This dedicated secure device would help to shift the extra load of encryption and decryption from the other FortiMail gateways. Emails are transferred to the dedicated device the same way quarantined emails are transferred.

Case Studies

Case One: Financial Services Industry

Common requirements:

- Confidentiality: Financial services companies are required to protect any electronic communication that includes sensitive data, such as account numbers, location of account, social security numbers, customer names and/or addresses, etc.
- Preventing phishing threats: Users continue to face a barrage of fraudulent emails, looking to fool users into divulging account details and other personal information.
- Regulation: Many organizations are facing internal, as well as industry and government regulations for secure communication. For example, SOX section 404 compliance requires secure and authenticated delivery of email messages to ensure privacy and confidentiality.

FortiMail Benefits:

- Ease of use: Identity Based Encryption (IBE) ensures privacy by using the recipient and other random factors to create unique user-based keys. There is no need of certification and key management. No additional hardware or software to install. No user provisioning and pre-enrollment requirements.
- Multi-layered protection: Coupled with FortiGuard™ Labs' industry leading real-time security services, FortiMail provides complete multi-layered antivirus, antispam, antispyware, and antiphishing security protection with a performance that will not affect your users or delay their communications.
- Compliance: Pre-defined HIPAA, SOX, and GLB lexical dictionaries are customizable and are included on every FortiMail appliance.
- Data Leak Protection: Pre-defined "Smart Identifiers" intelligently detect the accidental or intentional loss of confidential or regulated data. You can choose to block messages containing data matching a range of patterns or create policies to enforce the encryption of messages carrying this data, such as Credit Card or Social Security Numbers. DLP aids in PCI/DSS and HIPAA compliance.
- Compatibility: Support for non TLS/SSL capable SMTP domains by utilizing TLS/SSL over HTTP (HTTPS). Sensitive messages sent to domains that do not support SMTP encryption will use HTTP encryption.
- Flexibility: Provide both Push and Pull secure mail delivery capabilities. Pull messages reside on the appliance, while Push messages reside in the recipient inbox.
- Cost effective: IBE is available on all FortiMail appliances and in any mode of operation without an extra license or fees. Integrated security with no per-user or per-mailbox pricing.

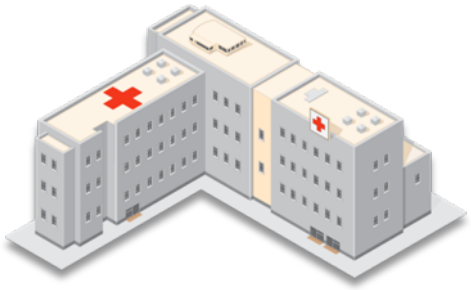
Deployment Example: A Medium-sized Financial Services Company in New England USA

This company was looking for secure email solutions to prevent its sensitive insurance policy and personal information from being exposed to unauthorized users, while maintaining usability. It also needed to prevent Data Leakage, such as Social Security Number, Credit Card strings, and Canadian SIN. Once detected, it wanted to encrypt this email before sending to large customers and partners. The customer didn't want to manage desktop email encryption solutions like PGP Desktop. It was also facing a budget constraint and didn't want to pay costly per-seat licensing.

Although the client had many questions about usability of Fortinet's IBE solution, the sales team was able to demonstrate exactly why IBE is so powerful and easy for the customer to use on a daily basis. This customer bought FortiMail because of the centralized administration, ease of use for the external encryption recipients, and SOX compliance. A single FortiMail 100C platform was deployed, and it processed approximately 20,000 messages per day. The project was so successful the customer decided to add another device to ensure High Availability.

Case Two: Healthcare Clinic/Hospital

Common requirements:



- Confidentiality: Patient information and medical data sent by emails, such as lab reports sent to a physician, emails from a doctor to another practitioner consulting for a second opinion, are private and highly sensitive.
- Regulation: HIPAA and similar regulations around the world require that healthcare providers ensure the confidentiality of patient information and medical record. Unauthorized disclosure of protected health information (PHI) is punishable by fines
- Extended use of IT: To mitigate financial risks many health care providers have resorted to faxing or post mails to deliver sensitive information which significantly increase operational costs.

FortiMail Benefits:

- DLP and Compliance: Pre-defined HIPAA, SOX, and GLB lexical dictionaries are customizable and on every FortiMail appliance. Automatically enforce privacy policies with PHI content scanning. Thanks to dictionaries or lexicon search that identifies PHI elements, FortiMail is able to detect and protect confidential information.
- Ease of use: FortiMail IBE is as easy to use as regular mail system. There is no need of certification and key management. No additional hardware or software to install. No user provisioning and pre-enrollment requirements. FortiMail allow leveraging mail as a means of health record communication.
- Automatically and manually triggered encryption: IBE can be triggered automatically when there is a policy match. Or the user can manually trigger IBE by specifying certain keywords in the message Subject or Body.
- Flexibility: Provide both Push and Pull secure mail delivery capabilities. Pull messages reside on the appliance, while Push messages reside in the recipient inbox.
- Cost effective: IBE is available on all FortiMail appliances and in any mode of operation without an extra license or fees. Integrated security with no per-user or per-mailbox pricing.

Deployment Example: A Medium-sized Health Insurance Company in US

This customer has a requirement to become HIPAA compliant, and secure all potentially sensitive information contained in outbound email messages, without the intervention of the senders. The customer also wishes to enable the internal users to manually trigger IBE.

A FortiMail-1000B is deployed as the last internal hop outbound and is configured to scan all outgoing messages for sensitive content or keywords specified by the company management. The customer takes advantage of the pre-defined HIPAA dictionary to enable its content monitoring policy. All potentially sensitive information is detected and secured. The automatic message encryption also occurs when a sender specifies certain keywords in the FortiMail system, such as "[secure]" or "[confidential]". For example, when a user puts [secure] in the message Subject or Body, the FortiMail will trigger IBE to encrypt the message automatically.

Summary

Businesses require secure mail delivery to meet policy requirements and provide a competitive advantage. Organizations are looking for alternatives to the certificate and key management challenges posed by existing solutions. They want an encryption solution that is easy to deploy and use and meets policy requirements for secure communications.

FortiMail IBE is as easy to use as standard email system--there is no need for certificate or key management for end-users, and no need to install additional hardware or software. A browser-based method allows the recipient to decrypt and read the secure message regardless of his operating system, mail client or user privilege. FortiMail enables organizations to eliminate the per-letter cost and environmental impact of paper-based communications, resulting in measurable cost savings. FortiMail IBE is an ideal secure email solution for healthcare, financial services, government and legal organizations with a need to meet compliance requirements.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
300 Beach Road #20-01, The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784